CTX711855 - Common SSL Error Messages and their Causes

This document was published at: http://support.citrix.com/kb/entry.jspa?externalID=CTX711855

Document ID: **CTX711855**, Created on: Nov 13, 2001, Updated: Jul 28, 2004

Products: ICA Win32 Program Neighborhood Client, Citrix Secure Gateway 1.1, Secure Gateway for MetaFrame 2.0

This document explains some SSL-related error messages that might be returned by an ICA Client when attempting to connect to a MetaFrame server or published application using SSL.

Error message:
"SSL security contact is invalid or expired (SSL 15)."

Reason:
Upgrade to client version 6.30.1050 or greater for the Win32 ICA Client.

Error message:
“Cannot connect to the citrix MetaFrame server. There is no route from the Citrix SSL Relay to the specified subnet address (SSL error 37).”

Reason:
CTX103203 – Citrix SSL Relay: SSL error 37 - Event IDs 10123 10112

Error message:
"The Remote SSL peer sent a bad certificate alert. (SSL Error 49)."

Reason:
Upgrade to client version 6.20.142 for the Macintosh.

Error message:
"The remote SSL peer sent an unrecognized alert (SSL Error 55)....Error : 132"

Reason:
The SSL Error 55 is caused by an invalid (or missing root) certificate..

Error message:
"Security alert: The name on the security certificate does not match the name of the server (SSL error 59)."

Reason:
The ICA Client is attempting to connect to the server using its NetBIOS name, IP address, or a fully-qualified domain name (FQDN) that does not match the subject of the server's certificate. To connect successfully, the ICA Client must connect using the DNS name of the server exactly as it appears on the server certificate. In NFuse scenarios, you must set AddressResolutionType=dns or dns-port in nfuse.conf and enable DNS name resolution on the farm properties panel in the Citrix Management Console. For more information about DNS name resolution, see page 65 of the *Administrator's Guide for MetaFrame XP with Feature Release 1*.

Error message:
"The server certificate received is not trusted (SSL error 61)."

Reason:
1. The required CA Root certificate is not installed on the client device. If you are using a well-known public certification authority such as Verisign, Baltimore, Thawte, or RSA, the required root certificate already exists on the client devices running a recent copy of Windows. However, if you are using your own certificate server to generate server certificates, or if you are using a trial certificate from a CA, you need to install the CA Root certificate on all client devices for them to connect. For more information about CA Root certificates and why they are necessary, read the white paper entitled Using the Citrix SSL Relay.

2. If your server certificate was issued by an intermediate certification authority, the Win32 ICA Client version 6.20.985 will not connect using SSL.. This is a client-side issue that affects the 32-bit ICA Client Version 6.20.985 connecting through the Citrix SSL Relay Service or Citrix Secure Gateway. This issue is resolved in versions 6.20.986 and later of the Win32 ICA Client. Download the latest version from the following URL: http://www.citrix.com/download/win-downloads.asp

Error message:
"The connection was rejected. The SSL certificate is no longer valid. Please contact your Citrix Administrator (SSL error 70)."

Reason:
The server certificate installed on your MetaFrame server is not yet valid or has expired. SSL server certificates typically have a fixed set of valid dates, and both the client devices system clock and the server's system clock must be set to a time that falls within that range for an SSL connection to succeed. (A common problem encountered when using Microsoft Certificate Services to generate digital certificates in-house is that the period of validity may not begin until the day after the certificate is generated.) To determine the validity date of your server certificate, double-click the certificate file and inspect the **Valid from** and **Valid to** fields.

Error message:
"One or more of the root certificates in the keystore are not valid(SSL error 73)."

Reason:
While not confirmed to resolve the issue, the Macintosh root certificate was determined to be in a CER format. Mac certificates need to be in a DER format with an extension of ".crt".

Or

On the Macintosh, the root certificate has been copied properly to the keystore/cacerts folder, but the user is receiving the above SSL Error when trying to connect. (See CTX104638 for resolution)

Error message:
"The Citrix SSL Server you have selected is not accepting connections."

Reason:
The Citrix Servers default port number was changed from 1494. Ensure ipv4-port address resolution is configured on the NFuse server. Apply CSGE110W001. Check wfclient.ini for the proper ProxyType=Auto setting. Use other standard troubleshooting methods, such as telnet, to ensure port 1494 is open between the client and server.